

Modems – The Overlooked Threat

Everything old is new again. When you're discussing overlooked security threats to your organization, don't forget to mention modems. Nearly every new PC shipped includes a modem, yet the security emphasis is on the threat *du jour*: war-driving, bluejacking, or inadequate mobile security, for example. At Sandstorm Enterprises, we understand that phones and modems are both a vital part of your business infrastructure and a potential avenue of attack.

Sandstorm Enterprises makes PhoneSweep[®], a telephone system security audit tool that searches for and identifies modems, fax machines, and other devices attached to telephone lines. PhoneSweep can identify security risks such as unsecured modems and potential vulnerability to toll fraud.

Why Worry About Modems?

The presence of unsecured, misconfigured, or unauthorized modems attached to computers on your network can undermine the most detailed security plan. People may set up modems accessible with no password or an easily guessed password. These modems are vulnerable to *wardialers*, black-hat hackers who call numbers systematically until they find a phone number that connects to an unsecured dialup access.

If a computer with a rogue modem is connected to your organization's network, anyone with a little computer skill and malicious intent can use that modem to access your network. Firewalls don't protect against this type of attack. The intruder gains access via phone lines, bypassing the firewalls that protect your organization's network borders.

It is in your organization's best interests to find rogue modems and shut them down before an attacker finds the breach in your security perimeter.

An Ethical War Dialer

Before the introduction of PhoneSweep in 1998, there were no commercial-quality tools for conducting telephone system security audits. Security professionals who wanted to find unsecured modems had to resort to using the same tools as the wardialers — publicly available programs written by amateur programmers, designed to commit illegal acts. These tools were generally unsupported, difficult to use, and had limited reporting capabilities. Furthermore, they sometimes contained "undocumented features" such as viruses or spyware. PhoneSweep was designed and written specifically as a commercial security audit tool by an experienced team of engineers and security professionals. It was designed to be easy to use, flexible, and powerful.

Ethical Use of PhoneSweep

PhoneSweep is a powerful tool, and any powerful tool can potentially be misused. Scanning phone numbers or looking for vulnerabilities in phone systems you are *not* authorized to scan is almost certainly illegal in your jurisdiction. However, organizations can easily and legally audit their *own* phone systems, scanning every number for unauthorized devices and tracking down any surprising results.

To further secure PhoneSweep, Sandstorm Enterprises provides a hardware license management device that must be attached to the computer before running the program. This device protects PhoneSweep from unauthorized use — no dialing can happen when the device is not attached.

Why Choose PhoneSweep?

When you choose PhoneSweep, you choose solid commercial-quality software, continuously updated and improved since its first product release in 1998. Security personnel in hundreds of organizations have chosen to give PhoneSweep a place in their security audits because it delivers results. Whether your organization has only 1,000 phone lines or over 10,000, PhoneSweep can help secure them. PhoneSweep's patented dialing technology and precision in discovering vulnerable modems is now relied on in over 80 countries.

Everything Old...

In the rush to provide security for today's Gigabit and wireless networks, it's easy to forget that the lowly modem can still be a threat to your "secure" network. You can mitigate that threat for existing modems by putting a strong security audit policy in place, and including PhoneSweep on your list of auditing tools.

...Is New Again

PhoneSweep is still in active development, with improvements and changes being released each year. As of version 5.4 (released in May 2006), PhoneSweep could identify over 460 remote-access systems, including dialup remote access servers, voice messaging systems, terminal servers, callback systems, data logging systems, print servers, mail gateways, and telephone switches, among others. PhoneSweep systems are available installed on desktop, laptop, and rackmount systems, as well as a software-only option. For organizations with many branch offices, we offer PhoneSweep Gold, which can remotely initiate and manage scanning activities.

All these options make it easy to obtain a PhoneSweep package that will fit your organization's security auditing needs. Modems may be "old news", but a security breach via a rogue modem could still cost your company in lost assets, leaked information, stolen intellectual property, and embarrassing press coverage. Visit our web site at <http://www.sandstorm.net/products/> for more information on PhoneSweep, or call us directly at 781-333-3200.